

UNITED STATES COURT OF APPEALS
FOR DISTRICT OF COLUMBIA CIRCUIT

MAR 24 2004

IN THE UNITED STATES COURT OF APPEALS
FOR THE DISTRICT OF COLUMBIA CIRCUIT

RECEIVED

ELOUISE PEPION COBELL, et al.,

Plaintiffs-Appellees,

v.

GALE A. NORTON,
Secretary of the Interior, et al.,

Defendants-Appellants.

No. 04-5084

[Civil Action No. 96-1285 (D.D.C.)]

**EMERGENCY MOTION FOR STAY PENDING APPEAL
AND FOR TEMPORARY STAY PENDING CONSIDERATION OF MOTION**

INTRODUCTION AND SUMMARY

Defendants-appellants the Secretary of the Interior, et al., respectfully ask this Court to stay pending appeal the preliminary injunction entered by the district court on March 15, 2004, insofar as it requires disconnection from the internet of computers and computer systems connected as of that date. We also ask that the Court enter a temporary stay while it considers our motion.¹

The injunction requires that the Department of the Interior immediately disconnect its computer systems from the internet. To avoid contempt, the Department has undertaken steps to comply with the order immediately. As a result, the most basic agency functions, including procurement, financial management, and hiring, are critically impaired. Databases accessed daily by thousands of members of the public have been taken off-line. The Department can no longer provide internet education services to children of Indian tribes.

The injury to the public and the government is significant and immediate. In contrast, there exists absolutely no evidence that the systems taken off-line as a result of the March 15 order pose any threat of harm of any kind. The purported purpose of the injunction is to obtain absolute security

¹Pursuant to Local Rule 8, plaintiffs' counsel has been given advance notice, by telephone, of the filing of this motion.

for data pertaining to money or property held in trust for individual Indians. Of the approximately 100,000 computers operated by the Department, only 6,600 house or provide access to Individual Indian Trust Data (IITD). Of those 6,600 computers, approximately 5,500 have been disconnected from the Internet for over two years. The many thousands of computers disconnected as a result of the March 15 order are those which the court had long since approved as either secure or neither housing nor providing access to IITD.

In ordering the disconnection of these computers, the court not only acted without evidence of harm, but failed even to provide notice as required by Fed.R.Civ.P. 65. That the district court nevertheless ordered that Interior computers be disconnected immediately underscores the extent to which the order does not seriously purport to weigh the relative harms at issue.

The injunction allows IT systems "essential for the protection against fires or other threats to life or property" to remain connected to the internet, provided that the court accepts certifications filed on March 22, 2004.² But Interior can avail itself of this limited exception only by incurring still wider disruption of its communications. As discussed below, to keep these systems on-line, Interior must physically disconnect thousands of its computers not only from internet access but from access to other computers within the Department (including e-mail), thus fundamentally undermining the Department's operations.

A district court order requiring that a federal agency disconnect itself from internet capability would be extraordinary under any circumstances. It is even more extraordinary in the absence of any evidence warranting an injunction. It is made more extraordinary still by the absence of any legal basis for the court's ruling. This is an action to compel an accounting under the American Indian Trust Fund Management Reform Act, Pub. L. No. 103-412, 108 Stat. 4239 (1994) (the "1994 Act"), This Court, in 2001, largely affirmed a declaratory judgment holding that the accounting had been unreasonably delayed under APA standards. However, in approving the district court's exercise of

² The order also allows National Park Service (NPS), the Office of Policy Management and Budget (OPMB), and the United States Geological Survey (USGS) to remain connected.

continuing jurisdiction, the Court specifically admonished that the only legal breach at issue was the failure to provide a timely accounting and that the court's jurisdiction would be limited to determining whether steps taken in preparation of that accounting might be "so defective" as to constitute additional unreasonable delay. Cobell v. Norton, 240 F.3d 1081, 1106, 1110 (D.C. Cir. 2001). The 1994 Act makes no reference to computer security and provides no measure of what security should be deemed adequate. Nothing in the statute or in this Court's decision permits the court to sever the agency's electronic communications to promote data security.

The district court's lack of authority is underscored by the enactment in November 2003 of Pub. L. No. 108-108. Responding to a September 2003 "structural injunction" issued by the district court (and later stayed by this Court), Congress provided that no principle of law "shall be construed or applied to require the Department of the Interior to commence or continue historical accounting activities * * * ." Inasmuch as the only legal basis claimed for the preliminary injunction here is that it bears some relation to plaintiffs' claim for an accounting, the court acted with an absolute lack of authority.

The government has appealed the district court's previous preliminary injunction regarding Interior's computers (No. 03-5262). That appeal is being briefed on an expedited schedule, with the government's opening brief due on April 6, 2004. (The government's separate brief in the structural injunction appeal, No. 03-5314, is due on the same date.) Because the district court – despite the pendency of the appeal – purported in its March 15 order to "supersede" and "replace" the order on appeal in No. 03-5262, the government, by separate motion, is asking that this appeal be consolidated with No. 03-5262, maintaining the existing briefing schedule. By proceeding on this highly expedited basis, any hypothetical harm resulting from a stay will be minimized, and, in the interim, sweeping harm and wholly unwarranted injury to government operations and the public will be avoided.

The government filed a notice of appeal and an emergency stay motion in district court on March 22, 2004 together with certifications required by the preliminary injunction to maintain connections for systems essential to protecting life or property. Because of the extraordinary impact

of the injunction, we are filing this motion now to avoid any delay in this Court's review if the district court does not grant an immediate stay.

STATEMENT

I. The Underlying Litigation for an Accounting.

The 1994 Act provides that "[t]he Secretary shall account for the daily and annual balance of all funds held in trust by the United States for the benefit of an Indian tribe or an individual Indian which are deposited or invested pursuant to the Act of June 24, 1938 (25 U.S.C. 162a)." Pub. L. No. 103-412, § 102(a).

Plaintiffs filed this class action in 1996 to require Interior to take actions with respect to individual Indian money ("IIM") accounts. The district court dismissed plaintiffs' common law trust claims, but allowed their suit to go forward because plaintiffs' "statutorily-based claims against the government can be brought under the APA." Cobell v. Babbitt, 91 F. Supp. 2d 1, 29 (D.D.C. 1999). This Court largely affirmed the declaratory judgment, concluding that agency action had been improperly delayed under APA standards. Cobell v. Norton, 240 F.3d 1081, 1108-09 (D.C. Cir. 2001). The Court explained, however, that the only actionable breach of duty was the failure to produce an accounting, and required the district court to amend its order to the extent that it purported to exercise jurisdiction over other related duties such as the management of computer systems. Id. at 1106. The Court stressed that the choice of how an accounting should be conducted was properly left to the agency, id. at 1104, and admonished the district court "to be mindful of the limits of its jurisdiction," id. at 1110, explaining that its jurisdiction was confined to determining whether future steps taken by Interior were so defective that they would "necessarily delay rather than accelerate the ultimate provision of an adequate accounting," ibid.

In Cobell v. Norton, 334 F.3d 1128 (D.C. Cir. 2003), the Court reversed a judgment of contempt that had been based in part on the district court's conclusion that the Secretary of the Interior had failed to initiate a historical accounting. Id. at 1150. (Based on its contempt trial the district court had declared that "Secretary Norton and Assistant Secretary McCaleb can now rightfully take their place * * * in the pantheon of unfit trustee-delegates." 226 F. Supp.2d at 161.)

This Court observed that "in her first six months in office Secretary Norton took significant steps toward completing an accounting," *id.* at 1148, including the creation of the Office of Historical Trust Accounting which had "'made more progress ... in six months [July through December, 2001] than the past administration did in six years.'" *Ibid.*

In September 2003, the district court issued a "structural injunction" that purported to assert control over virtually all accounting and trust operations to be overseen by a Monitor and agents with unlimited powers of access. 283 F. Supp. 2d 66. Congress responded by enacting new legislation. The Conference Committee explained that the court-ordered accounting would cost between six and twelve billion dollars, H.R. Conf. Rep. 108-330, at 117, and "would not provide a single dollar to the plaintiffs[.]" *Ibid.* Pub. L. No. 108-108 provides that "[N]othing in the American Indian Trust Management Reform Act of 1994, Public Law 103-412, or in any other statute, and no principle of common law, shall be construed or applied to require the Department of the Interior to commence or continue historical accounting activities with respect to the Individual Indian Money Trust," absent new legislation or the lapse of Pub. L. 108-108 on December 31, 2004.

This Court has stayed the structural injunction pending appeal. *See* No. 03-5314.

II. The Computer Security Issue and The July 2003 Preliminary Injunction.

A. In connection with its 1999 ruling, the district court appointed Alan Balaran as Special Master to oversee certain discovery issues. Mr. Balaran subsequently assumed a much expanded role, and the government in October 2003 filed in this Court a petition for a writ of mandamus seeking the disqualification of Mr. Balaran under 28 U.S.C. § 455. *See* No. 03-5288 (scheduled for oral argument on April 8, 2004).³

On November 14, 2001, Special Master Balaran issued a Report and Recommendation Regarding the Security of Trust Data at the Department of the Interior, which identified deficiencies

³ Several non-party individuals have also filed for mandamus relief seeking Mr. Balaran's disqualification with respect to contempt proceedings concerning them. *See* No. 03-5047 and related cases (argued March 15, 2004). On March 15, 2004, this Court in the latter matter issued an order staying the portion of the district court's September 17, 2002 order referring to Mr. Balaran various contempt matters regarding non-party individuals. *See* Order, No. 03-5047 (Mar. 15, 2004).

in the security of Interior's IT systems that the Master believed could detrimentally affect the integrity of Individual Indian Trust Data. On one or more occasions in 2001 and later, the Master believed he had uncovered such deficiencies because computer specialists retained by him were able with some success to "hack" into an Interior system. Following the issuance of the Master's report, the district court on December 5, 2001 entered a temporary restraining order that required Interior to disconnect from the internet all systems housing IITD.

In response, Interior agreed to a Consent Order, issued on December 17, 2001, by which it agreed to a procedure for restoring internet connections. The Consent Order provided that offices would be restored to the internet upon agreement by the Master that the systems were secure or that they provided no access to IITD. Pursuant to the Consent Order, Interior reconnected to the internet systems which did not house or did not provide access to IITD. Interior also reconnected to the internet several systems which were adequately secure from unauthorized access. The reconnected systems housing or providing access to IITD included the Minerals Management Service, the Inspector General, the Bureau of Land Management, and the National Business Center. Other systems housing or providing access to IITD, including the Bureau of Indian Affairs and the Office of Special Trustee, remained offline.

Although the Master's Report and the Consent Order provide the background to the present injunction, the Consent Order was stayed by the July 28, 2003 preliminary injunction (and the March 15, 2004 preliminary injunction) and is not at issue here.

B. Efforts to reconnect remaining systems fell victim to a dispute between Interior and the Special Master concerning the Special Master's plan to conduct "penetration testing" of systems reconnected pursuant to the terms of the Consent Order. After Interior and the Special Master were unable to resolve this dispute, plaintiffs moved for a temporary restraining order and a preliminary injunction on the ground that Interior's refusal to allow the Special Master to conduct penetration testing posed an imminent threat to IITD.

On July 28, 2003, the district court entered a preliminary injunction (Exh. 2). The injunction obviated the Master's further participation in determining the extent to which Interior may

communicate electronically with the public. Under the terms of the July 28, 2003 injunction, the court assumed full authority over internet access.

In assuming control over the Department's computer systems, the court treated all Interior computers as presumptively subject to disconnection without regard to whether a particular system had already been reconnected because it was secure or did not house or access IITD. The order required Interior immediately to disconnect from the Internet all IT systems that house or access IITD.

Although the injunction purported to require immediate disconnection, it did not in fact do so. The injunction included a procedure that delayed its full impact. Interior was allowed to submit certifications showing that the systems still connected to the internet were either "essential for protection against fires or other threats to life or property" or that these systems either did not house or access IITD or were secure from Internet access by unauthorized users. With regard to the systems that were already disconnected, Interior was required to file a proposal "setting forth a method of approving individual reconnections of disconnected Interior computer systems, and of determining whether the Reconnected Systems should stay reconnected."

In issuing the July 28 preliminary injunction, the court considered no evidence of harm resulting from the systems that already been reconnected to the internet. Nor did it consider evidence of harm that would result from reconnecting the computers off-line. The government has appealed from the ruling, in No. 03-5262.

C. On August 11, 2003, Interior filed the certifications required under the July 2003 injunction. A variety of Interior officials provided certifications, under penalty of perjury, that specific systems either did not house or provide access to IITD or were secure from Internet access by unauthorized users. Later, Interior filed a proposal setting forth a method of approving individual reconnections of disconnected Interior computer systems, and of determining whether reconnected systems should stay reconnected. Plaintiffs filed responses to Interior's submissions within the times set forth in the injunction.

The district court did not rule at that time on Interior's certifications or proposal of a method of approving disconnected systems and, accordingly, no new systems were disconnected. In effect, therefore, the July 28, 2003 injunction temporarily preserved the status quo as it then existed. In the following months there has been no indication that the security of any IITD has been compromised.

III. The District Court's March 15, 2004 Shutdown Order.

On March 15, 2004, without holding any additional evidentiary hearing, the district court issued a preliminary injunction rejecting Interior's certifications and its proposal for approving reconnection of systems already off-line (Exh. 1). Although the government's certifications had been pending before the court since the previous August, the order required Interior immediately to disconnect all IT systems from the Internet, whether or not they house or access IITD. The court allowed IT systems "essential for the protection against fires or other threats to life or property" to remain connected to the Internet, subject to the requirement that Interior provide sworn declarations within 5 days "specifically identifying any and every such Information Technology System that has remained connected to the Internet and setting forth in detail the reasons Interior believes such Information Technology System to be essential for the protection against fires or other threats to life or property." In addition, the court also allowed systems in the custody and control of the NPS, the OPMB, and the USGS to remain connected because the court was satisfied that these bureaus do not house or access IITD.

The district court did not base its injunction on any new evidence that the security of IITD had been compromised or was in imminent jeopardy. Instead, the court declared that Interior's certifications pursuant to the July injunction were procedurally inadequate. The court believed, in particular, that the certifications did not comply with 28 U.S.C. § 1746 and LCvR 5.1(h) because they stated that "I declare under penalty of perjury that the foregoing is true and correct to the best of my knowledge, information, and belief." The court was of the view that the declarations were defective because they used the words "to the best of my knowledge, information, and belief." Op. 9-11.

The court identified the harm justifying the disconnection of thousands of computers as follows. The court reasoned that because the "Special Master ceased his monitoring activities in July 2003," it had "no assurance that even those systems previously reconnected by the Special Master are secure." Op. 25. The court stated that "many of Interior's IT systems are connected to each other, and an Internet connection to an IT system that does not house individual Indian trust data itself but is operated by a bureau that has another IT system that does house or access individual Indian trust data might allow unauthorized access to the IT system housing individual Indian trust data through the connections between systems." Ibid. On this basis, the court concluded that "the continued connection to the Internet of any IT system that may not itself house individual Indian trust data but is operated by a bureau within Interior that has custody or control over another IT system that does house or access individual Indian trust data constitutes further and continuing irreparable injury to Plaintiffs." Id. at 25-26.

The court dismissed the impact of disconnections on the government and the public. The court stated that Interior would "no doubt continue to suffer some hardship and inconvenience as a result of having systems disconnected from the Internet," but concluded that "such hardship is outweighed by the potential alteration or destruction of IIM trust data by unauthorized access through the Internet." Op. 26. And, because "those systems necessary to protect U.S. citizens against the threat of fire, or any other threat to life or property will remain connected to the Internet," the court concluded that the "interest of the three hundred thousand plus current beneficiaries of the individual Indian trust outweigh the potential inconvenience of those parties that would otherwise have access to Interior's Internet services." Ibid.

ARGUMENT

I. THE INJUNCTION IS WITHOUT BASIS IN LAW OR FACT.

A. The Injunction Is Wholly Without Basis In Law.

In an age in which internet communication has become as integral as the telephone, the district court has required a cabinet agency to eliminate its electronic connections to the world. No provision of law vests the district court with that authority.

The only statute at issue in this suit is the 1994 Act. As relevant here, the statute provides that Interior should provide a daily and annual accounting for Individual Indian Money accountholders. The statute does not authorize courts to destroy the communications networks of federal agencies. Indeed, it does not even reference computer security. The statute neither provides a measure for determining what security is adequate nor empowers a court to effect agency-wide disconnections to achieve whatever level of security it believes appropriate.

The court's exercise of power is without basis in the statute and is flatly at odds with this Court's initial decision in this case. In reviewing the declaratory judgment issued in 1999, this Court concluded that the district court had subject matter jurisdiction under the APA "to compel agency action 'unlawfully withheld or unreasonably delayed.'" 240 F.3d at 1095. Although the district court had already dismissed plaintiffs' common law claims, the Court further required the district court to amend its ruling to reflect the fact that the only "actual legal breach" at issue "is the failure to provide an accounting, not [the] failure to take the discrete individual steps that would facilitate an accounting." *Id.* at 1106. The Court admonished the district court "to be mindful of the limits of its jurisdiction," *id.* at 1110, noting that the only basis for retaining jurisdiction over the case was to determine whether Interior's actions "would necessarily delay rather than accelerate the ultimate provision of an adequate accounting * * *." *Ibid.*

Nothing in the 1994 Act or this Court's initial decision could conceivably be construed to afford a basis for requiring the Department of the Interior to remove itself from the internet. If any doubt on that score existed, it was removed by the passage of Pub. L. No. 108-108 in November 2003. That statute provides that nothing in any law "shall be construed or applied to require the Department of the Interior to commence or continue historical accounting activities * * *." Congress has undoubted authority to amend the substantive law that provides the basis for forward-looking relief. *See, e.g., Miller v. French*, 530 U.S. 327, 344 (2000); *Plaut v. Spendthrift Farm, Inc.*, 514 U.S. 211, 232 (1995); *Robertson v. Seattle Audubon Soc'y*, 503 U.S. 429, 432-35, 441 (1992). It has done so here. The only asserted basis for the preliminary injunction here is its purported relation to an accounting. *See op. 2* (the IT security issues addressed in the preliminary injunction are "a

corollary" to Interior's statutory responsibility under the 1994 Act to provide an accounting). Pub. L. No. 108-108 deprives the court of any basis for ordering accounting activities and relief claimed to be attendant on a duty to perform accounting activities.

In sum, the district court acted without authority in severing Interior's electronic communications.

B. The Injunction Is Without Basis In Fact.

As discussed, to avert a permanent injunction requiring Department-wide disconnection, the government agreed, in December 2001, to a consent order that would allow reconnection of computers that the Special Master agreed provided no access to ITTD or otherwise posed no threat to ITTD security. Although the vast majority of Department computers were reconnected, the Special Master would not agree to the connection of some systems, including the computers servicing the Office of the Special Trustee and the Office of Hearings and Appeals. When the government was unwilling to accept new demands by the Master regarding "penetration testing," the consent order mechanism broke down entirely.

The July 2003 injunction superseded the consent order. One part of the order required the continued disconnection of computers off-line but afforded a mechanism for approving their restoration. However, the order further declared that all systems would be disconnected unless Interior submitted and the court approved new certifications. In issuing that injunction, the court cited no evidence that the systems connected to the internet had created actual or imminent threats to ITTD data.

In issuing the March 15 injunction, the court likewise considered no evidence of actual or imminent harm, despite the fact that it had ample opportunity to conduct a hearing in the seven months since Interior submitted its certifications. As discussed, the court did not even provide notice as required by Fed.R.Civ.P. 65.

It is unclear why the district court felt free to ignore the most basic requirements of fairness reflected in the governing rules. To the extent that the March 15 order is a new injunction that "supersedes" the previous ruling, the court was plainly required to afford the hearing required by the

rules. If the court believed it was modifying the injunction already on appeal, serious questions exist about its jurisdiction to do so in a way that alters the status quo. And principles of equity would certainly require that a court provide notice and opportunity to be heard when it radically "modifies" the effect of an injunction more than half a year after its issuance.

In any event, no evidence supports the issuance of an injunction, and the court fundamentally erred in refusing even to consider the extensive certifications demonstrating the lack of basis for any further disconnections.

In response to the July 2003 injunction, Interior officials had submitted voluminous certifications, under penalty of perjury, explaining in detail why various computer systems posed no risk to IITD security. The court refused even to consider these certifications, which had been pending before it since the previous August, on the ground that the certifications were purportedly "procedurally" invalid. Each of the government's certifications stated that "I declare under penalty of perjury that the foregoing is true and correct to the best of my knowledge, information, and belief." The court concluded that this language deviated from the requirements of 28 U.S.C. § 1746 and LCvR 5.1(h) because they included the words "to the best of my knowledge, information, and belief." Op. 9-11.

By their terms, 28 U.S.C. § 1746 and LCvR 5.1(h) apply only where "under any law of the United States or under any rule, regulation, order, or requirement made pursuant to law, any matter is required or permitted to be supported * * * by the sworn declaration, verification, [or] certificate . . . of [a] person" (emphasis added). No statute, regulation or rule required the "certifications" here to be executed under oath, and the district court cited none. Moreover, both the statute and the local rule provide that a certification meets applicable requirements if it is "substantially" in the form of the language set forth in those provisions, *i.e.*, "I declare (or certify, verify, or state) under penalty of perjury that the foregoing is true and correct." A declaration or certification "to the best of" the declarant's knowledge, information, and belief is plainly sufficient under the statute and the rule, and also under the requirements of Federal Rule of Civil Procedure 56. *See United States v. Roberts*, 308 F.3d 1147, 1154-55 (11th Cir. 2002), cert. denied, 123 S. Ct. 2232 (2003) (false statement

attested to as "correct and true to the best of my knowledge and belief" was substantially in the form provided by § 1746); Colon v. Coughlin, 58 F.3d 865, 872 (2d Cir. 1995) (reversing summary judgment against plaintiff because verified complaint "attesting under the penalty of perjury that the statements in the complaint were true to the best of his knowledge" was sufficient under Rule 56).

The court's ruling is additionally inexplicable because the July 2003 injunction required only that the certifications made to the court were to comply with Rule 11 of the Federal Rules of Civil Procedure. See 7/28/03 PI Order, ¶ B.1(b) (Exh. 2). Rule 11 governs the signing of pleadings, not evidentiary submissions by witnesses, and nothing in the Rule would, in any event, support the imposition of the requirement now announced by the court. To the contrary, insofar as the Rule is relevant at all, it provides that "[e]xcept when otherwise specifically provided by rule or statute, pleadings need not be verified or accompanied by affidavit." Fed. R.Civ.P. 11(a). No rule or statute imposes a specific requirement of this kind with respect to the certifications submitted to the district court here pursuant to the July 2003 order. And, of course, Rule 11 explicitly contemplates a certification standard based on "knowledge, information, and belief." Fed. R. Civ. P. 11(b).

Even if the district court's understanding of the applicable formal requirements were not fundamentally mistaken, it could not properly have severed the communications of an executive agency on this basis. If the court's understanding were correct, the proper course would have been to permit the government to amend its declarations, not to destroy its communications systems.

2. The district court devoted one paragraph to the substance of the 900 pages of materials submitted to the court. In so doing, the court noted an inconsistency regarding the status of the Automated Fluid Minerals Support System (AFMSS). Op. 11-12. The certification indicated that the AFMSS had been re-connected. However, a table attached to the applicable report indicated that the system was not connected. The information in the table was, in that respect, outdated. To comply with the July 2003 injunction, the government was required to assemble its detailed certifications within two weeks. That a court would disconnect an agency's communications systems on the basis of a single item of outdated information is extraordinary.

In the discussion in its opinion, the court also cited three government reports addressing broad questions of IT management and security. Op. 17-24. The court did not directly rely on these reports, which provide no information as to the security of IITD.

The court cited a report of a congressional subcommittee giving Interior a grade of "F" for its overall computer security. Op. 22 (citing House Committee on Government Reform, Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census, "2003 Federal Computer Security Report Card"). But computer security includes a wide range of issues, including physical facilities security, personnel qualifications and training, and protections against data loss.⁴ From this general perspective, the report also issued overall grades of "F" for computer security to the Departments of Justice, State, Energy, Homeland Security, Health and Human Services, Agriculture, and Housing and Urban Development. Nothing in the subcommittee's scorecard even remotely addressed the particular question of the threat to the integrity of data posed by unauthorized internet access, much less whether any such threat might exist with respect to Individual Indian Trust Data.

The court also cited an Interior report to OMB entitled "Financial Management Status Report and Strategic Plan (FY2004-FY2008)," issued in September 2003. See Op. 17. Again, no part of this report was focused on the particular question of unauthorized access to data via the internet, much less the question of such unauthorized access to IITD. Indeed, the court's brief discussion of the report dwells on issues pertaining to financial management and compliance with accounting standards. See id. at 18.

A September 12, 2003 GAO report entitled "Information Technology: Department Leadership Crucial to Success of Investment Reforms at Interior" likewise offers no evidence of any

⁴The court misapprehended this basic point in criticizing the government for failing to provide a "uniform" IT security metric here. See Op. 13-14. While there are various government standards dealing with aspects of computer security in general, there is, as Interior's certifications explained, no uniform method of measuring whether a system is fully "secure" from the threat of unauthorized access to data via the internet. See Declaration of Associate Deputy Interior Secretary James Cason at pp. 5-6 (Aug. 11, 2003) (Exh. 5).

demonstrable threat to IITD. The report deals with Interior's overall management of its IT projects. It lends no support to the proposition that unauthorized access through the internet presents any imminent danger to the integrity of individual Indian trust data. See Op. 20-22.

The general issues of IT security faced by Interior and other Cabinet agencies are manifold, and Interior has committed significant resources to their resolution. The certifications that Interior submitted to the court pursuant to the July 28, 2003 preliminary injunction explained in detail the measures that had been put in place to protect IITD from unauthorized internet access. The government's showing included twelve separate certifications, with hundreds of pages of supporting attachments. For the Court's information, we attach, as an example, the declaration of Associate Deputy Interior Secretary James Cason that formed part of the Department's August 2003 filings. Nothing in the government reports cited by the district court casts any doubt on the accuracy of the agency's account.

II. THE BALANCE OF HARMS WARRANTS AN IMMEDIATE STAY.

The government seeks emergency relief with respect to the disconnections required by the March 15 order. The stay will thus preserve the status quo as of that date. The disconnections effected by the March 15 order concern the computers that even the Special Master had approved for internet connection. As discussed, absolutely no evidence exists that the systems on-line as of March 15 had compromised any IITD in any way or that such harm was imminent. Indeed, there is no evidence that anyone other than the Special Master has ever "hacked" into any system housing or providing access to IITD data.

The court observed that Interior would "no doubt continue to suffer some hardship and inconvenience as a result of having systems disconnected from the Internet." Op. 26. That characterization in no sense reflects the reality of its ruling.

The Department of the Interior is a massive organization that performs a vast array of critical functions on behalf of the American people. No one would suggest that the Department could carry out its mission without access to the telephone. It is unclear why the district court believed that Department-wide disconnection from electronic communication would result in mere

"inconvenience." As Secretary Norton notes in her declaration attached hereto, "[t]he Department is integrated into the web of electronic communications as fundamentally as the telephone system. Internet communication is not merely a useful tool – it is essential to much of what we do." Norton Decl., p.1 (Exh. 3).

The significant and immediate harm resulting from the injunction is outlined in detail in the attached declaration of Interior's Chief Information Officer, Mr. W. Hord Tipton (Exh. 4). The Declaration provides a far from exclusive list of the ways in which the injunction undermines Interior's ability to carry out fundamental operations and to provide service to the public:

- Contracting and Procurement. Interior averages more than 50 procurement announcements per business day on requirements that exceed \$4 billion per year. A government-wide regulation requires that all such procurement actions be electronically posted on a single point of entry through GSA (the General Services Administration). The court's injunction seriously hinders this process, undermining the Department's ability to post notices for millions of dollars in contracts involving critical and time-sensitive matters. At least one of Interior's acquisition programs provides acquisition services throughout the government, and involves contracts for goods and services not only within the United States but in other countries as well. Tipton Decl., p.3.
- Financial Management. Internet connectivity is critical to the systems used in performing Interior's financial accounting, funds control, management accounting, and financial reporting, and in preparing the Department's financial statements. Tipton Decl., p.4. As with its procurement processes, Interior's financial management activities affect a host of other government agencies as well; an Interior financial accounting, control, and reporting system is also used by roughly a score of non-Interior entities. Ibid.
- Education Programs. The injunction disables many programs that directly benefit Indians. For example, the Department of the Interior operates an extensive school

system for the benefit of tens of thousands of individuals, in hundreds of institutions, spread across more than twenty states. Many of the facilities involved are located in remote parts of the country, where their scholastic programs cannot operate without computer access and communications via the internet. Tipton Decl., p.6.

- Royalties Distribution. Each month the Minerals Management Service (MMS) receives, processes, and disburses over \$500 million in mineral revenues derived from federal and Indian leased lands. Among the beneficiaries of these royalty payments are at least 41 Indian tribes. The processes for handling and distributing these monies are heavily reliant on automated systems and access to the internet, and the court's shutdown order will make it difficult if not impossible for significant sums to be allotted and paid in a timely and accurate manner. Tipton Decl., p.7.
- IT Security. Ironically, the injunction impairs IT security itself. The Department's IT security program depends on the internet to download anti-virus software and other critical "patches." Tipton Decl., p.8. The injunction thus threatens to prevent Interior not only from making improvements but even from maintaining and preserving its existing IT security profile.
- Hiring and Recruitment. Under the court's March 15 order, Interior's web-based personnel system for hiring and recruitment will grind to a halt. Tipton Decl., pp.6-7.
- Public Data Bases. The Bureau of Land Management (BLM) maintains case status for all public domain lands, which consist of approximately 270 million acres and an additional 500 million acres of subsurface minerals. The Public Information Data System (PIDS) is a huge electronic repository of publicly available document images, consisting of documents such as geophysical and geological permits, plans of exploration and development, and drilling permits. The Office of Surface Mining administers the Technical Innovation and Professional Services (TIPS) database containing critical information pertaining to mines, including technical designs, permitting information, and subsidence data. State regulatory authorities access TIPS

approximately 135 times each day. Millions of people who use the internet to learn about and plan visits to the nation's national wildlife refuges every year will be prevented from doing so. Tipton Decl., pp.5-6.

Finally, as the Tipton Declaration explains, the consequences of the injunction are even broader than those specifically directed by the court, and will undermine intra-Department communications as well as communications between Interior and the public. To maintain an internet connection for portions of systems necessary to protect against fires and other threats to life or property, Interior will be forced to reconfigure its IT systems in ways that will drastically affect the effectiveness of those systems. The computers used for these essential services are linked to the internet through a series of connections that are shared by computers devoted to services that are not essential in this sense. To maintain the internet link for "essential" systems and also sever all internet links for "nonessential" systems, the Department must physically disconnect from all communications access thousands of laptops and personal computers not directly used for functions essential to protect against fires and other threats to life and property. As a result, the employees who use those computers will be unable to communicate electronically within the Department as well as outside the Department. Tipton Decl., p.2.

In sum, an emergency stay is necessary to avoid irreparable harm to the government and the public. Issuance of a stay will result in no harm of any kind. By separate motion we are asking that the appeal from the March 15 order be consolidated with our appeal from the July 2003 order docketed as No. 03-5262. The government's brief, due on April 6, 2004, will fully address the issues arising from both rulings.

CONCLUSION

This Court should issue a stay of the district court's March 15, 2004, preliminary injunction pending appeal insofar as it requires disconnection of computers and computer systems connected to the internet as of that date. The Court should also issue a temporary stay while it considers the stay application and plaintiffs' response.

Respectfully submitted,

PETER D. KEISLER
Assistant Attorney General

ROSCOE C. HOWARD, JR.
United States Attorney

ROBERT E. KOPP
MARK B. STERN
THOMAS M. BONDY
CHARLES W. SCARBOROUGH
ALISA B. KLEIN
(202) 514-5089

Thomas M. Bondy
A
Attorneys, Appellate Staff
Civil Division, Room 9108
Department of Justice
601 D Street, N.W.
Washington, D.C. 20530

MARCH 2004

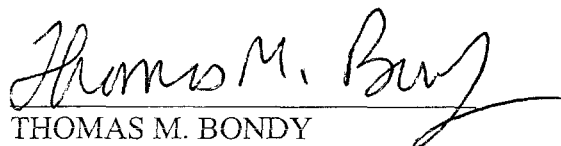
A D D E N D U M

(Certificate as to parties and amici)

CERTIFICATE AS TO PARTIES AND AMICI

Pursuant to Circuit Rules 8 and 28(a)(1)(A), the undersigned counsel certifies that the named plaintiffs-appellees in this class action are Elouise Pepion Cobell; Mildred Cleghorn; Thomas Maulson; and James Louis Larose. Earl Old Person is no longer a named plaintiff but remains a member of the class. The class consists of present and former beneficiaries of Individual Indian Money accounts, excluding those who had filed their own actions prior to the filing of the complaint in this case.

Defendants-Appellants are Gale A. Norton, as Secretary of the Interior; Aurene M. Martin, as Acting Assistant Secretary of Interior-Indian Affairs; and John W. Snow, as Secretary of Treasury.


THOMAS M. BONDY

CERTIFICATE OF SERVICE

I hereby certify that on this 24th day of March, 2004, I caused copies of the foregoing motion to be sent to the Court and to the following by hand delivery:

The Honorable Royce C. Lamberth
United States District Court
United States Courthouse
Third and Constitution Ave., N.W.
Washington, D.C. 20001

Keith M. Harper
Native American Rights Fund
1712 N Street, N.W.
Washington, D.C. 20036-2976
(202) 785-4166

and to the following by federal express, overnight mail:

Elliott H. Levitas
Law Office of Elliott H. Levitas
1100 Peachtree Street
Suite 2800
Atlanta, GA 30309-4530
(404) 815-6450

and to the following by regular, first class mail:

Dennis Marc Gingold
Law Office of Dennis Marc Gingold
607 14th Street, N.W., Box 6
Washington, D.C. 20005

Earl Old Person (pro se)
Blackfeet Tribe
P.O. Box 850
Browning, MT 59417


THOMAS M. BONDY